TECHNOLOGY REPORT

セキュリティ編

:DeNA

株式会社ディー・エヌ・エー

CONTENTS

1 まえがき P.3～

2 セキュリティサマリー P.5～
- 2-1 基本方針
- 2-2 セキュリティポリシー
- 2-3 DeNAのセキュリティの強み

3 セキュリティ向上に対する取り組み P.10～
- 3-1 セキュリティ組織体制
- 3-2 個人情報管理組織体制
- 3-3 DeNA CERT
- 3-4 プライバシー保護
- 3-5 海外のプライバシー法令への対応
- 3-6 研修／人材育成

4 セキュリティ施策 P.17～
- 4-1 データセキュリティ
- 4-2 外部からの不正アクセス対策
- 4-3 脆弱性対応
- 4-4 クラウド設定の自動管理
- 4-5 入退室管理

5 セキュリティ業界への貢献 P.23～
- 5-1 業界への情報発信
- 5-2 セキュリティツールのオープンソース化

01

まえがき

世の中に届けるDelightに安心・安全を提供する。

DeNAグループは、ゲーム、ライブコミュニティ、スポーツ、ヘルスケア／メディカルを中心とした多岐にわたる事業を展開し、それぞれの特徴を融合させつつ、お客さま一人ひとりに想像を超えるDelightを届けています。

お客さまにDelightを感じていただくためには、体感のよい優れたサービスが不可欠であると同時に、安心・安全にご利用いただくためのセキュリティ基盤も重要です。昨今ではその安心・安全を脅かす「サイバー攻撃」や「情報漏えい」等にまつわるニュースを毎日のように耳にします。脅威は高まる一方です。

DeNAグループでは、プライバシーおよびセキュリティを重要な経営戦略と位置づけ、「お客さまからお預かりしている情報の適切な保護」ならびに「提供サービスおよび社内システムをセキュアに保つ」ことを情報セキュリティに係る基本方針として掲げ、安心かつ安全なサービスの提供に取り組んでいます。

セキュリティは、組織面、人的面、技術面などの基本的な対策の積み重ねが非常に大事であると考えています。その基本的な対策をDeNAらしく技術と仕組みを駆使しして強化に努めています。強化に必要な仕組みは自ら開発することもあります。そのために知見の蓄積、技術力も磨きます。
これがDeNAセキュリティの考え方であり強みと言っても過言ではありません。

IT本部セキュリティ部 部長　岡村 隆行

02

セキュリティサマリー

すべてのサービスに、
安心と安全を。

基本方針

DeNAグループでは、一人ひとりに想像を超えるDelightを届けるため、インターネットやAIを活用して様々なサービスを提供しています。

しかしこれらのサービスは特性上、サイバー攻撃やプライバシー侵害に関する脅威に晒されていることから、当社では「お客さまからお預かりしている情報の適切な保護」ならびに「提供サービスおよび社内システムをセキュアに保つ」ことを情報セキュリティに係る基本方針として掲げ、安心かつ安全なサービスの提供に取り組んでいます。

「想定外の出来事」を予測して、「想定内の対策」としてアップデートし続ける。

セキュリティポリシー

DeNAグループでは、基本方針として掲げた「お客さまからお預かりしている情報の適切な保護」「提供しているサービスおよび社内システムをセキュアに保つ」ことを実現するために、適用される法令等の順守だけではなく、サイバーセキュリティ経営ガイドライン、NIST（米国国立標準研究所）サイバーセキュリティフレームワークなどを参考としたグループ統一的なセキュリティポリシーを整備しています。

対応方針の原則を示した「DeNAグループ情報セキュリティポリシー」を中心に、情報資産の適切な取り扱いを具体的に示した「グループ情報管理スタンダード」、情報システムの開発、運用に組み込むべきセキュリティ対策を具体的に示した「グループ情報システムスタンダード」を整備／順守することで安心、安全の提供に努めています。

しかしながら、サイバー攻撃などの脅威は日々高度化しています。よって、内外環境の変化を掴み、適時セキュリティポリシーのアップデートをし続けています。

DeNAだからできる安心安全のための全力コミット。

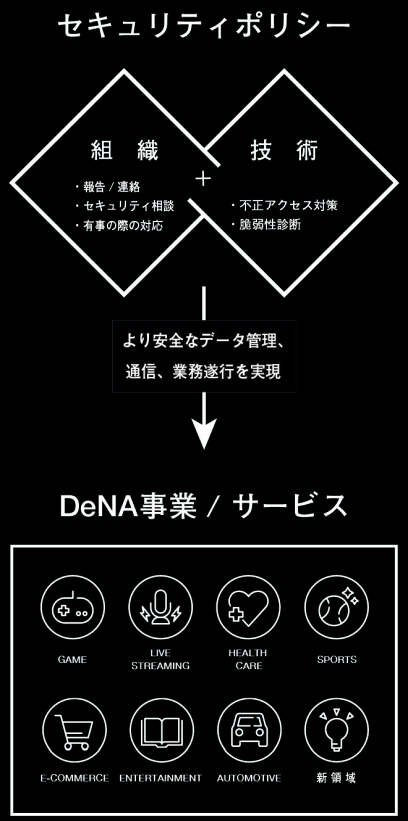
セキュリティポリシーに実効性を持たせる取り組みも必要です。

組織と技術の側面からセキュリティ施策を事業に適用していくために、セキュリティ部を中心としたセキュリティ対策チーム（DeNA CERT）を編成し、平時から有事に至るまでの取り組みを進めています。

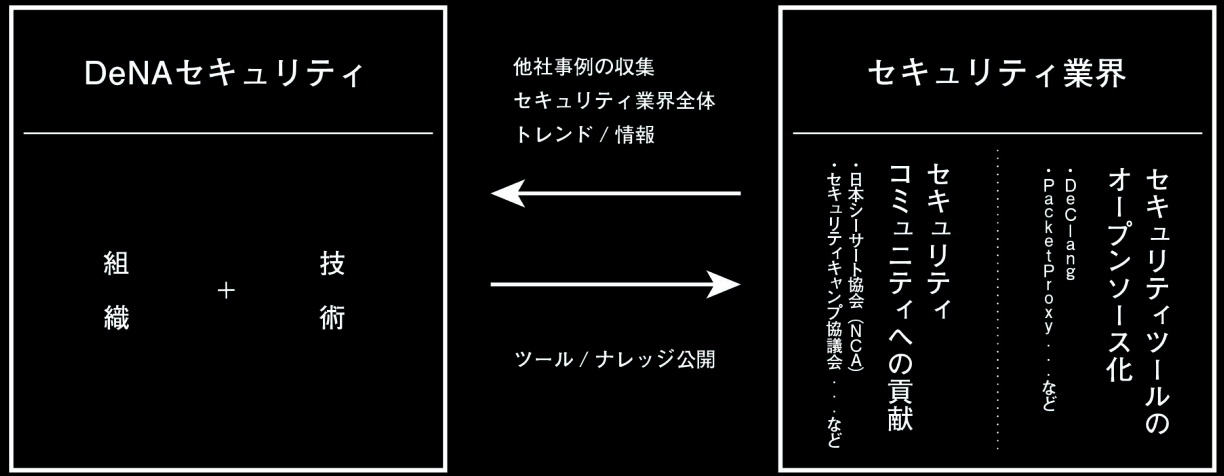
商用のセキュリティ対策ソフトも使用しますが、DeNAの高基準なセキュリティポリシーに則った強固なセキュリティを施すためには、それだけでは不十分です。事業特有の課題に対応し、その上で高いセキュリティレベルを実現するために、必要な機能を自社開発し、サービス開発・運用に利用しています。

特にスマホアプリの脆弱性診断やハッキング対策を中心に、DeNAのセキュリティエンジニア部隊は世の中の常識に囚われることなく、診断技術や防御機能を自社開発して事業のセキュリティレベルを向上させています。

これらのセキュリティの仕組みが、より安心安全な事業活動、サービスの提供を実現しています。



DeNAで培われたツールとナレッジを セキュリティ業界全体へ。



セキュリティ対策はDeNAだけの問題ではなく、IT化していく社会全体で取り組む必要があります。DeNAグループで培われたナレッジは、社外のコミュニティにも共有しています。また、セキュリティの研究・開発で出来上がった診断ツール等をオープンソースとして公開し誰もが利用できるようにすることで、業界全体のセキュリティレベル向上にも貢献しています。

03

セキュリティ向上に対する取り組み

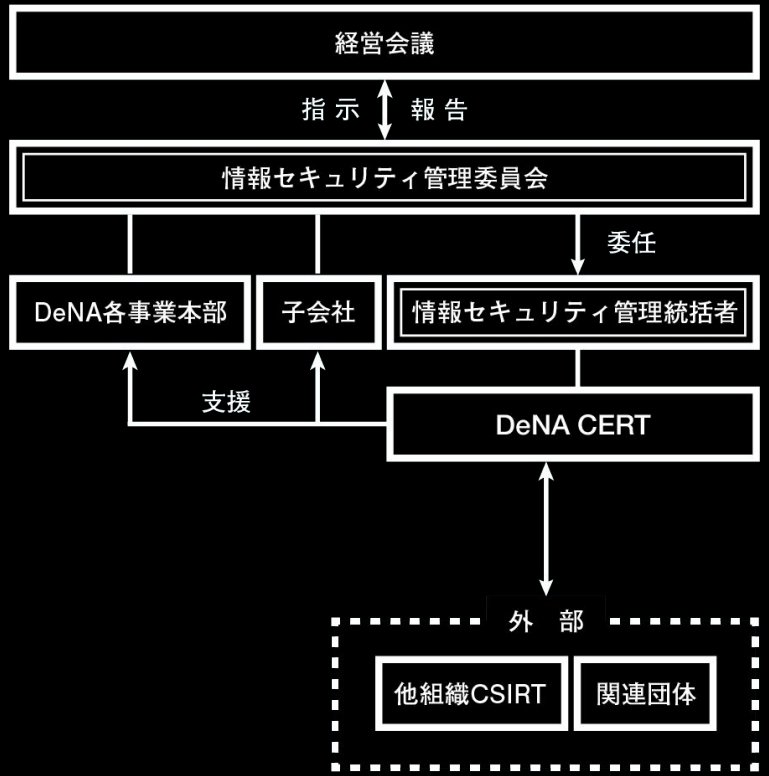
強固なセキュリティは、組織構造から。

情報セキュリティ 管理委員会

DeNAグループでは代表取締役社長を委員長とする情報セキュリティ管理委員会を設置し、グループ横断的な体制を整備しています。同委員会での議論は定期的に経営会議に報告し、重要な事項は経営会議でも議論しています。更に重要な事項は取締役会にも報告しています。

情報セキュリティ管理統括者

DeNAグループの情報セキュリティ管理業務を統括する者として、情報セキュリティ管理委員会から情報セキュリティ管理統括者が任命されています。情報セキュリティ管理統括者は、DeNA CERTをリードし、セキュリティ課題及び対策の向上に取り組んでいます。



* CSIRT（シーサート）：Computer Security Incident Response Teamの略称。セキュリティインシデント対応チーム。

プライバシー保護にも、しっかりとした体制を。

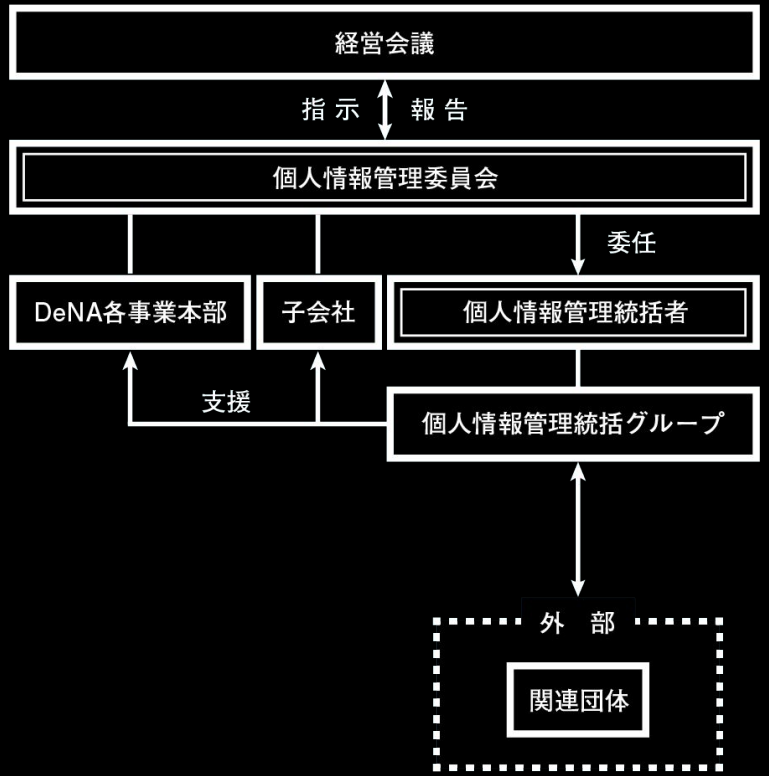
個人情報保護にも、セキュリティ対策と同様の体制を取り入れています。

個人情報管理委員会

DeNAグループでは代表取締役社長を委員長とする個人情報管理委員会を設置し、グループ横断的な体制を整備しています。同委員会での議論は定期的に経営会議に報告し、重要な事項は経営会議でも議論しています。更に重要な事項は取締役会にも報告しています。

個人情報管理統括者

DeNAグループの個人情報管理業務を統括する者として、個人情報管理委員会から個人情報管理統括者が任命されています。個人情報管理統括者は、個人情報管理統括グループをリードし、DeNAグループにおける個人情報の適切な取り扱いの確保に努めています。



サービスを支える
セキュリティ対策チーム。

DeNA CERT

ディー・エヌ・エー サート / DeNA Computer Emergency Response Team

セキュリティ部を中心とした複数の部署からなる横断的なセキュリティ対策チームです。

平時においても事業部門と連携し、セキュリティポリシーの浸透に努め、最新のセキュリティ対策を実施し、安心安全なサービス提供に尽力しています。

万が一インシデントの恐れが生じた場合には、DeNA CERTが中心となり対応します。専門性の高いメンバーが在籍しているため、迅速に対応することが可能です。

また、外部のコミュニティにもセキュリティ関連の情報を発信しており、社内外のセキュリティ対策の向上に努めています。

お客さま情報の安全な保護に尽力しています。

プライバシー保護

DeNAグループは、お客さまのプライバシーに関する権利を尊重しています。様々なサービスにてお客さまの個人情報を取得していますが、予め利用目的を明示した上で、お客さまの個人情報を取り扱っています。

個人情報については、必要最小限の情報のみの取得、アクセス権限の最適化、利用目的を達成した情報の消去等の個人情報の適切な取り扱いに努めています。また、個人情報管理台帳を全社で整備し、取得から消去に至るまでの取り扱いを可視化しています。

詳細はDeNAプライバシーポリシー（ https://dena.com/jp/privacy/ ）をご確認ください。

サービスを世界中に提供するため、
海外のプライバシー法令の対応に取り組んでいます。

海外のプライバシー法令への対応

海外のお客さまにサービスを提供する場合は、GDPR（EU一般データ保護規則）をはじめ、サービスを提供する国のプライバシー関連法令に対応する必要があります。

DeNAグループでは、法務部門とセキュリティ部門で構成された海外プライバシー事務局にて、法令調査からセキュリティ対策までワンストップで事業部門をサポートしています。

セキュリティルールの周知と対応の徹底。

従業者研修

DeNAグループは、従業者一人ひとりがセキュリティに関するルールをしっかり守り、十分な配慮をして業務ができるよう、DeNAグループの全従業者（派遣、協力会社社員等を含む）を対象に個人情報および情報セキュリティに係る研修を実施しています。提携先企業様の未公開情報等を取り扱う者に対しては、情報にアクセスする前に専用の研修を実施しています。

セキュリティ人材の育成

現在、サイバーセキュリティに関する脅威が多様化・高度化しており、これに対応するためのセキュリティ人材の育成の必要性も指摘されています。
セキュリティ部員が、あらゆるケースに迅速に対応できるよう、サイバー攻撃の特性に合わせた攻撃シナリオを仮定し、定期的にインシデント対処の訓練を実施するなど、業務を通じて必要なセキュリティ知識が得られるように環境整備しています。セキュリティツールの開発やオープンソース化についても、セキュリティ知識の向上の施策としても捉えています。

タイミング	内　容	対　象
入社時 / 業務開始時（月 次）	・情報セキュリティ研修 ・個人情報研修	・全従業者 （派遣、協力会社を含む）
	・エンジニア向け セキュリティ研修	・すべてのエンジニア （派遣、協力会社を含む）
年　次	・情報セキュリティ研修 ・個人情報研修	・全従業者 （派遣、協力会社を含む）
	・役職者向け情報 セキュリティ研修	・すべての役職者
四半期	・経営会議での セキュリティ情報共有会	・役員 ・グループエグゼクティブ
役職就任時	・役職者向け情報 セキュリティ研修 ・役職者向けインシデント対応 ワークショップ	・新たに役職者に就任した者

04

セキュリティ施策

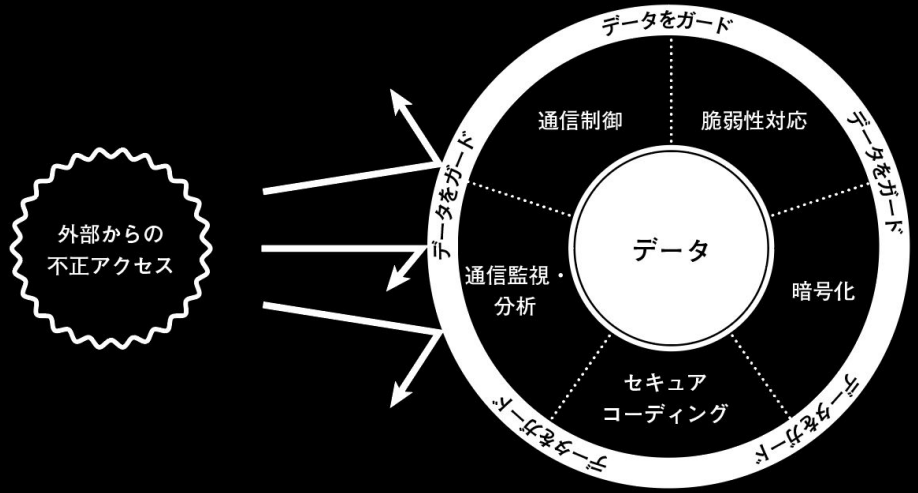
すべてのデータに機密度を設定し、機密度に応じて適切な管理に取り組んでいます。

データセキュリティ

特にお客さま個人を特定できるデータは、高度な暗号化を適切に施した上で、アクセスを制限しています。アクセス制限については、アカウントを一元的に管理できる仕組みを導入し、統合管理しています。また、アクセスした記録を残すことでトレーサビリティ（いつ、どこで、誰が扱ったのか分かること）を確保しています。

※ヘルスケア事業において、ゲノム解析業務および要配慮個人情報を扱う業務などについては、上記に加えてデータへのアクセス経路を限定し、かつ操作画面を録画する施策等も導入しています。

様々な脅威に対し、多層的な手段を用意し、リスクを低減しています。



DeNAグループでは、攻撃シナリオを踏まえた不正アクセス対策を導入しています。業務上不要な通信の制御、通信の監視・分析、脆弱性対応、セキュアコーディング、及びデータの項目単位での暗号化など、多層防御を実施することで、リスクを低減しています。特に脆弱性対応、暗号化については、内製化しており、事業サービスの特性に合わせて、より高いセキュリティレベルを実現しています。

危険性を1つでも多く減らすために、DeNAだからできること。

脆弱性対応

DeNAグループでは、提供するサービスの脆弱性を適切に対処することも重要だと考えています。DeNAグループでは社内のセキュリティエンジニアが知見を持ち、脆弱性対応を実施できる体制を持っているため、自社に即した深度ある診断を必要なタイミングで速やかに行うことができます。脆弱性診断ツールも自ら開発し、診断の質を常に向上させています。また、DeNAグループ以外の企業からも脆弱性対応のご相談を受けることもあります。特にスマホアプリに対する脆弱性対応やハッキングからの防衛は発展途上の分野ですが、DeNAのセキュリティエンジニア部隊は世の中の常識に囚われることなく診断技術や防御機能を自社開発して事業のセキュリティレベルを向上させています。また、それらの研究・開発過程で出来上がった診断ツール等をオープンソースとして公開し誰もが利用できるようにすることで、業界全体のセキュリティレベル向上にも貢献しています。

* 脆弱性：プログラムの不具合や設計上の不備によって発生する、ソフトウェアのセキュリティ上の欠陥。

膨大なチェックを自動化させて、小さな人的ミスも減らします。

クラウド設定の自動管理

DeNAグループでは、クラウド技術を活用してサービスを開発・運営しています。主にAmazon Web Services（AWS） ／ Google Cloudを多数利用しています。

クラウドサービスでは設定ミスが情報漏えい等を引き起こす恐れがあります。そこで、AWS、Google Cloudについては、それぞれの具体的な設定手順を定めたガイドラインを作成し、エンジニア等に周知していますが、人が設定するためにどうしてもミスは発生します。よって、設定値を毎日、自動的に監視し、ミスがあれば通知する仕組みを自ら開発することで、サービスの品質を高めています。

オープンな社風でも、すべてのドアを全員が開けられる訳ではありません。

入退室管理

DeNAグループでは複数の拠点を有していますが、セキュリティカードおよび監視カメラによって入退室を管理しています。

さらに、ゲーム事業における提携先企業様の秘匿情報、お客さまとのやり取りを行うカスタマーサポート業務、およびヘルスケア事業におけるお客さまの機微情報など特に重要な情報を取り扱う執務室においては、当該業務専用の執務室を準備し、執務室の全景を記録する監視カメラの導入、関与する者のみ入室権限を付与するなど、より厳格な入退室管理を実施しています。

05

セキュリティ業界への貢献

セキュリティ業界への貢献、外部との情報交換活動を実施しています。

日本シーサート協議会

幹事会員として、他組織のセキュリティ担当者を繋ぎ、問題を解決する場を提供しています。

これらの活動を通じ、当社自身も同業他社、他業種の様々なCSIRTと利害関係を超えてセキュリティに関する情報交換、相互協力を行い、社内外のセキュリティ向上に役立てています。

https://www.nca.gr.jp/

* CSIRT（シーサート）：Computer Security Incident Response Teamの略称。セキュリティインシデント対応チーム。

セキュリティキャンプ協議会

会員企業として、若年層の優秀なセキュリティ人材の早期発掘と育成を目標とした「セキュリティ・キャンプ」の普及、運営に貢献しています。

https://www.security-camp.or.jp/

サイバー防災

インターネット事業会社と通信事業会社によるインターネット上の防災意識の啓発を目的とした取り組みに参加しています。

わかりやすい啓発コンテンツを提供し、インターネットの安心安全な使い方を学ぶことに貢献しています。

https://www.cyber-bousai.jp/

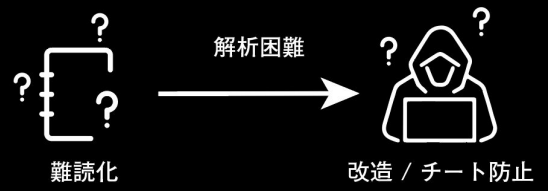
※上記以外においても、自社で培ったノウハウを、外部のセキュリティセミナー等で積極的に発信しています。DeNAグループだけではなく、社会全体のセキュリティレベルの向上に貢献しようと日々努力を続けています。

DeNAグループ内のみならず、業界全体のセキュリティ技術の水準向上に取り組んでいます。

セキュリティツールのオープンソース化

DeClang

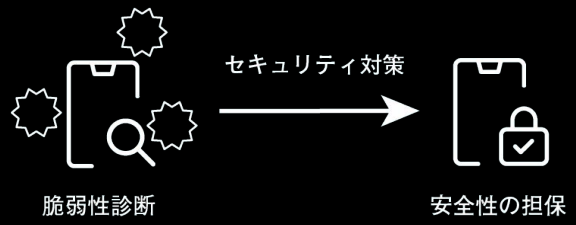
スマホゲームのチート対策コンパイラ



Androidアプリなどにおいて、リバースエンジニアリング（仕様解析）を困難にすることで、改造／チートを防止する難読化ツール。
https://github.com/DeNA/DeClang

PacketProxy

脆弱性診断ツール



万が一、通信の内容を不正に改ざんされた場合に、サーバ、または、クライアント側で異常(バグ／脆弱性)が発生しないかテストするツール。複数社にご利用いただいております。
https://github.com/DeNA/PacketProxy

本資料について

本資料は、2024年7月時点の情報に基づき作成しております。
今後、DeNAグループ内の組織変更やご提供するサービスの多様化、また社会情勢や経済の変動など、
様々な観点から総合的に判断したうえで、本資料に記載している体制や仕組みなどの変更を行う場合があります。

お問い合わせ先

以下からお問い合わせください。
https://dena.com/jp/contact/

株式会社ディー・エヌ・エー